

Traffic Analysis – Decrypting HTTPS Malware Traffic

Date: August 1, 2025

Tool Used: Wireshark

Focus: Encrypted Traffic Analysis (HTTPS) | Malware Identification |
Network Forensics

Analysed a packet capture (PCAP) from a Dridex malware infection on a Windows 10 machine. All web traffic was encrypted via HTTPS (TLS), and no session key or key log file was provided. The objective was to extract meaningful indicators and identify malicious behaviour without decrypting payloads.

Key Findings

Encrypted Communication:

Despite TLS encryption, valuable indicators were extracted from SNI fields, IP patterns, and request metadata.

Infected Device:

Identified as 10.4.1.101 (hostname: DESKTOP-U54AJ8K) through repeated NBNS registrations and outbound activity.

Malware Activity:

Dridex malware confirmed via suspicious domain and HTTP requests such as GET /invest_20.dll

Analysis Screen Shots

Encrypted Traffic View (TCP Stream)



By following the TCP stream, we observe encrypted HTTPS traffic. At this point, the payload contents are unreadable, only encrypted data is visible. This indicates that malicious behavior may be hidden within encrypted channels.

Decrypted Traffic View (TLS Stream)



By following the TLS stream, partial decryption was possible using available session keys. While full payload content remained inaccessible due to incomplete certificate data, the process exposed some previously hidden HTTP requests within the encrypted traffic.

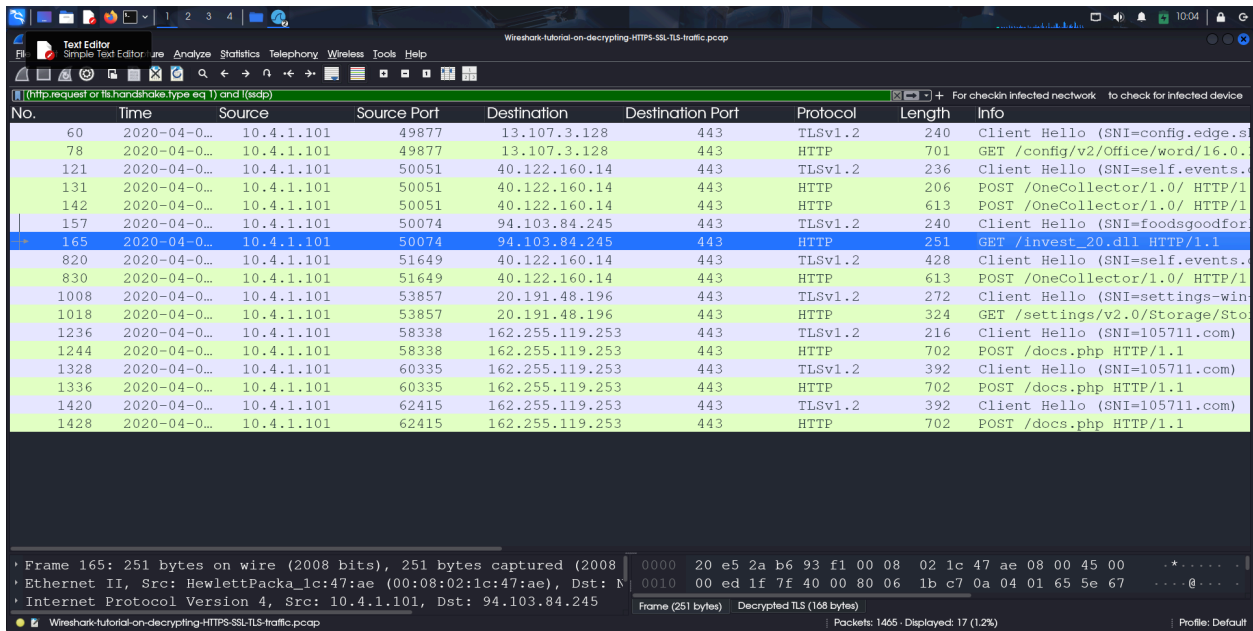
Malicious DLL File (Dridex Variant)

Analysis revealed a malicious DLL file, typical of Dridex variants that inject code into legitimate processes.

After decrypting the HTTPS traffic, HTTP requests to microsoft.com and skype.com were revealed, likely part of routine system processes.

However, the following malicious traffic indicates Dridex malware activity:

- GET /invest_20.dll
Captured in the screenshot as a direct HTTP request to download a malicious DLL payload used to trigger the infection.



| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Info |
|------|--------------|------------|-------------|-----------------|------------------|----------|--------|------------------------------------|
| 60 | 2020-04-0... | 10.4.1.101 | 49877 | 13.107.3.128 | 443 | TLSv1.2 | 240 | Client Hello (SNI=config.edge.s |
| 78 | 2020-04-0... | 10.4.1.101 | 49877 | 13.107.3.128 | 443 | HTTP | 701 | GET /config/v2/Office/word/16.0... |
| 121 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | TLSv1.2 | 236 | Client Hello (SNI=self.events.4 |
| 131 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | HTTP | 206 | POST /OneCollector/1.0/ HTTP/1 |
| 142 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | HTTP | 613 | POST /OneCollector/1.0/ HTTP/1 |
| 157 | 2020-04-0... | 10.4.1.101 | 50074 | 94.103.84.245 | 443 | TLSv1.2 | 240 | Client Hello (SNI=foodsgoodfor |
| 165 | 2020-04-0... | 10.4.1.101 | 50074 | 94.103.84.245 | 443 | HTTP | 251 | GET /invest_20.dll HTTP/1.1 |
| 820 | 2020-04-0... | 10.4.1.101 | 51649 | 40.122.160.14 | 443 | TLSv1.2 | 428 | Client Hello (SNI=self.events.4 |
| 830 | 2020-04-0... | 10.4.1.101 | 51649 | 40.122.160.14 | 443 | HTTP | 613 | POST /OneCollector/1.0/ HTTP/1 |
| 1008 | 2020-04-0... | 10.4.1.101 | 53857 | 20.191.48.196 | 443 | TLSv1.2 | 272 | Client Hello (SNI=settings-win |
| 1018 | 2020-04-0... | 10.4.1.101 | 53857 | 20.191.48.196 | 443 | HTTP | 324 | GET /settings/v2.0/Storage/Sto |
| 1236 | 2020-04-0... | 10.4.1.101 | 58338 | 162.255.119.253 | 443 | TLSv1.2 | 216 | Client Hello (SNI=105711.com) |
| 1244 | 2020-04-0... | 10.4.1.101 | 58338 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 1328 | 2020-04-0... | 10.4.1.101 | 60335 | 162.255.119.253 | 443 | TLSv1.2 | 392 | Client Hello (SNI=105711.com) |
| 1336 | 2020-04-0... | 10.4.1.101 | 60335 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 1420 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | TLSv1.2 | 392 | Client Hello (SNI=105711.com) |
| 1428 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |

Frame 165: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on interface 0
Ethernet II, Src: Hewlett-Packard, Dst: 94.103.84.245
Internet Protocol Version 4, Src: 10.4.1.101, Dst: 94.103.84.245
Hypertext Transfer Protocol GET /invest_20.dll HTTP/1.1

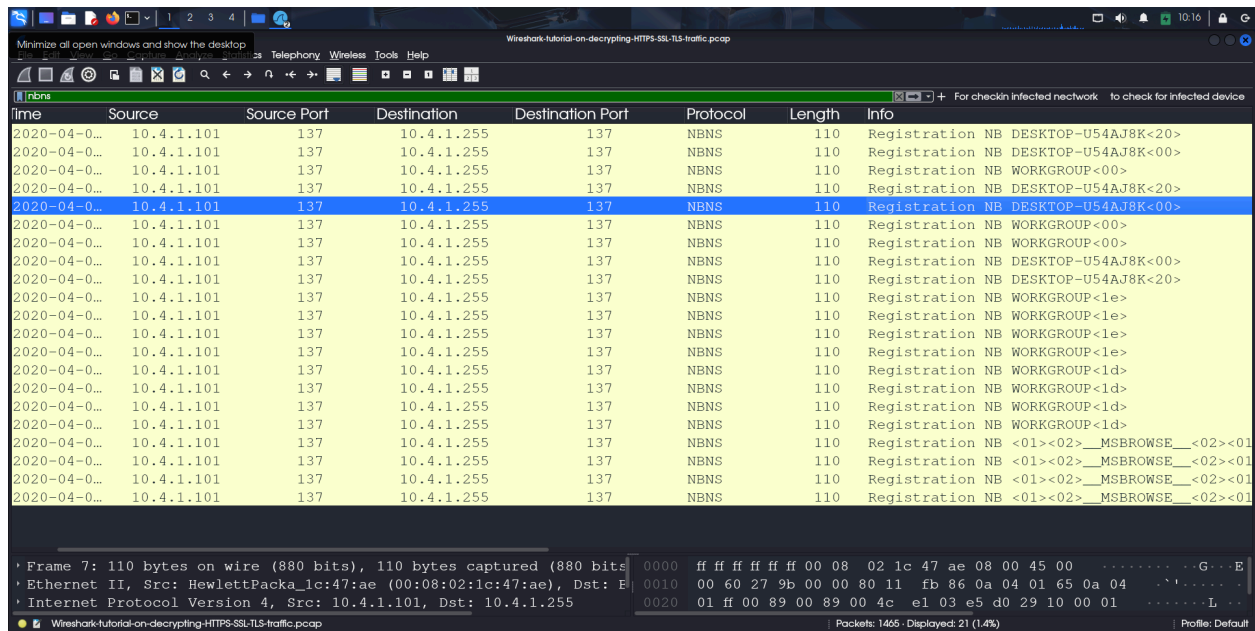


| No. | Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Info |
|-----|--------------|------------|-------------|-----------------|------------------|----------|--------|------------------------------------|
| 153 | 2020-04-0... | 10.4.1.101 | 49877 | 13.107.3.128 | 443 | TLSv1.2 | 240 | Client Hello (SNI=config.edge.s |
| 154 | 2020-04-0... | 10.4.1.101 | 49877 | 13.107.3.128 | 443 | HTTP | 701 | GET /config/v2/Office/word/16.0... |
| 155 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | TLSv1.2 | 236 | Client Hello (SNI=self.events.4 |
| 157 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | HTTP | 206 | POST /OneCollector/1.0/ HTTP/1 |
| 158 | 2020-04-0... | 10.4.1.101 | 50051 | 40.122.160.14 | 443 | HTTP | 613 | POST /OneCollector/1.0/ HTTP/1 |
| 159 | 2020-04-0... | 10.4.1.101 | 50074 | 94.103.84.245 | 443 | TLSv1.2 | 240 | Client Hello (SNI=foodsgoodfor |
| 160 | 2020-04-0... | 10.4.1.101 | 50074 | 94.103.84.245 | 443 | HTTP | 251 | GET /invest_20.dll HTTP/1.1 |
| 161 | 2020-04-0... | 10.4.1.101 | 51649 | 40.122.160.14 | 443 | TLSv1.2 | 428 | Client Hello (SNI=self.events.4 |
| 162 | 2020-04-0... | 10.4.1.101 | 51649 | 40.122.160.14 | 443 | HTTP | 613 | POST /OneCollector/1.0/ HTTP/1 |
| 163 | 2020-04-0... | 10.4.1.101 | 53857 | 20.191.48.196 | 443 | TLSv1.2 | 272 | Client Hello (SNI=settings-win |
| 164 | 2020-04-0... | 10.4.1.101 | 53857 | 20.191.48.196 | 443 | HTTP | 324 | GET /settings/v2.0/Storage/Sto |
| 165 | 2020-04-0... | 10.4.1.101 | 58338 | 162.255.119.253 | 443 | TLSv1.2 | 216 | Client Hello (SNI=105711.com) |
| 166 | 2020-04-0... | 10.4.1.101 | 58338 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 167 | 2020-04-0... | 10.4.1.101 | 60335 | 162.255.119.253 | 443 | TLSv1.2 | 392 | Client Hello (SNI=105711.com) |
| 168 | 2020-04-0... | 10.4.1.101 | 60335 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 169 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | TLSv1.2 | 392 | Client Hello (SNI=105711.com) |
| 170 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 171 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 172 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 173 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 174 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 175 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 176 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |
| 177 | 2020-04-0... | 10.4.1.101 | 62415 | 162.255.119.253 | 443 | HTTP | 702 | POST /docs.php HTTP/1.1 |

Frame 165: 251 bytes on wire (2008 bits), 251 bytes captured (2008 bits) on interface 0
Ethernet II, Src: Hewlett-Packard, Dst: 94.103.84.245
Internet Protocol Version 4, Src: 10.4.1.101, Dst: 94.103.84.245
Hypertext Transfer Protocol GET /invest_20.dll HTTP/1.1

Infected System Identified

The source IP 10.4.1.101 was repeatedly broadcasting NBNS traffic, identifying itself as DESKTOP-U54AJ8K.



The image shows a Wireshark packet capture window titled "Wireshark-tutorial-on-decrypting-HTTPS-TLS-traffic.pcap". The packet list on the left shows 21 packets, all of which are NBNS (NetBIOS Name Service) traffic. The selected packet (packet 7) is expanded, showing the following details:

| Time | Source | Source Port | Destination | Destination Port | Protocol | Length | Info |
|--------------|------------|-------------|-------------|------------------|----------|--------|---|
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<20> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<20> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<00> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB DESKTOP-U54AJ8K<20> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1e> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1e> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1e> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1d> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1d> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1d> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB WORKGROUP<1d> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB <01><02>_MSBROWSE__<02><01> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB <01><02>_MSBROWSE__<02><01> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB <01><02>_MSBROWSE__<02><01> |
| 2020-04-0... | 10.4.1.101 | 137 | 10.4.1.255 | 137 | NBNS | 110 | Registration NB <01><02>_MSBROWSE__<02><01> |

The packet details pane for the selected packet (Frame 7) shows the following information:

- Frame 7: 110 bytes on wire (880 bits), 110 bytes captured (880 bits) on interface 0
- Ethernet II, Src: Hewlett-Packard (08:00:02:1c:47:ae), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Internet Protocol Version 4, Src: 10.4.1.101, Dst: 10.4.1.255
- NetBIOS Name Service, Registration NB DESKTOP-U54AJ8K<20>

The packet bytes pane shows the raw data in hexadecimal and ASCII:

```
0000  ff ff ff ff 00 08 02 1c 47 ae 08 00 45 00  ...G...E
0010  00 60 27 9b 00 00 80 11  fb 86 0a 04 01 65 0a 04  ...L...
0020  01 ff 00 89 00 89 00 4c  e1 03 e5 d0 29 10 00 01  ...L...
```

Conclusion

Through partial decryption of TLS traffic using available session keys, limited visibility was gained into previously encrypted communications. Although full payload inspection wasn't possible, key indicators of compromise were uncovered. The infected device was observed communicating with suspicious endpoints, leading to the download of a .dll file, a common method for malware delivery. Follow-up POST requests further confirmed malicious activity consistent with Dridex behavior. This underscores the importance of encrypted traffic analysis in identifying infection stages, even when decryption is incomplete.